****

LABORATORY COMPUTER SERVICES SELF ASSESSMENT FEBRUARY 2006

****

Multiple solutions for laboratory information systems (LIS) exist. Traditional systems have a local "host" database (i.e., the computer hardware and software) serving the information needs of the laboratory; the laboratory is the only "user." In the current environment, the host is often physically remote from the laboratory and in fact the host may have multiple user laboratories. Many of the Computer Services questions may apply to host, user, or both, depending on how information services are organized in the laboratory. For laboratories which do not have host functions on site, the inspector should mark nonapplicable questions N/A. However, the laboratory is responsible for ensuring that the provider of host functions meets CAP requirements (see GEN.42165, below).

The questions in this section do NOT apply to the following:

1. *Desktop calculators*
2. *Small programmable technical computers*
3. *Purchased services such as the Quality Assurance Service or Laboratory Management Index Service of the College of American Pathologists*
4. *Micro computers used solely for word processing, spreadsheets, or similar single user functions*
5. *Dedicated microprocessors or workstations that are an integral part of an analytic instrument*

*****REVISED**** ***03/30/2005***

GEN.42165 **Phase II** **N/A**

If components of the LIS are located at a facility other than the one under this CAP accreditation number, is there evidence that the remote facility complies with CAP requirements for host LIS functions?

NOTE: This question does not apply if all components of the LIS are under the laboratory's CAP/CLIA-88 registration number. This requirement may be addressed by a copy of the CAP accreditation certificate from other sites, or evidence that the computer facility has been provided a copy of this Checklist, and has satisfactorily addressed the contents of the Computer Facility section, and all other pertinent items, with documentation provided to the laboratory director and the CAP inspector.

COMMENTARY:

N/A

GEN.42457 Phase II YES
In the judgment of the laboratory director, is the functionality and reliability of the computer system (hardware and software) adequate to meet the needs of patient care?

NOTE: Patient and laboratory data should be available online for a reasonable period of time, depending on the needs of the institution. The laboratory director is responsible for determining if the computer system reliability (hardware, software, and/or storage capacity) meets the patient care needs of the organization.

COMMENTARY:

N/A

COMPUTER FACILITY

This section applies to laboratories where the computer facilities are housed. If the computer facilities are located at another site, mark these 4 questions N/A and continue with the LIS/Computer Procedure Manual section.

GEN.42750 Phase I YES
Is the computer facility and equipment clean, well-maintained and adequately ventilated with appropriate environmental control?

NOTE: The computer facilities should be clean, well maintained, and in a location that is environmentally controlled, as required by the most restrictive vendor specifications.

COMMENTARY:

N/A

GEN.42800 Phase II YES historically from previous inspections, but Keith and Donald will check to make sure.

Is fire-fighting equipment (extinguishers) appropriate for electrical components available?

NOTE: Water based fire extinguishers should not be used.

COMMENTARY:

N/A

REFERENCE: Hoeltge GA, *et al.* Accidental fires in clinical laboratories. *Arch Pathol Lab Med.* 1993;117:1200-1204.

GEN.42850 Phase I YES
Are all wires and computer cables properly located and/or protected from traffic?

COMMENTARY:

N/A

*****REVISED** 03/30/2005***

GEN.42900 Phase II YES
Is the computer system adequately protected against electrical power interruptions and surges?

NOTE: Protection from electrical surges and interruptions must be adequate to prevent loss of data. An uninterruptible power system (UPS) or similar protective device (e.g., isolation transformer) must be considered. Periodic testing of this protective equipment to ensure protection of data and proper shutdown of computer equipment is considered best practice.

COMMENTARY:

N/A

LIS/COMPUTER PROCEDURE MANUAL

GEN.42950 Phase II YES - The DPH IT Staff is currently using the "SLI System Policies and Procedures" document that was written by UMMS-IT. The DPH IT Staff is currently revising this to include changes that resulted from the recent Network Migration.

Are LIS/computer procedures clearly documented, complete and readily available to all authorized users?

NOTE: Procedures should be appropriate to the level of use of the system, and must encompass the day-to-day activities of the laboratory staff as well as the daily operations of the Information Technology staff. It is not required for all procedures to be kept in a single manual, as long as the users have access to the procedures they need to perform their job duties. Current practice must match policy and procedure documents.

COMMENTARY:

N/A

*****NEW***** ***03/30/2005***

GEN.42975 Phase II YES - The DPH IT Staff is currently using the "SLI System Policies and Procedures" document that was written by UMMS-IT. The DPH IT Staff is currently revising this to include changes that resulted from the recent Network Migration.

Is there a procedure for the support of the computer system?

NOTE: The laboratory must have a procedure outlining the support of the system, including local maintenance, vendor support and emergency contact information.

COMMENTARY:

N/A

GEN.43000 Phase II YES they were approved by UMMS IT, but will be approved by Mark Thibault and the Network Staff here when they are finalized. Is there documentation that laboratory computer procedures are reviewed at least annually by the laboratory director or designee?

NOTE: A single signature on a title page or index of all procedures is not sufficient documentation that each procedure has been carefully reviewed. Signature or initials on each page of a procedure is not required.

COMMENTARY:

N/A

HARDWARE AND SOFTWARE

NEW* *03/30/2005*

GEN.43011 Phase II YES, this is kept track through the Help Desk System and Change Control Log used as part of the "SLI UMMS-DPH Physical Security Procedure".
Is there documentation of all hardware modifications?

COMMENTARY:

N/A

GEN.43022 Phase II YES, Sada and I keep track of this using the Change Control Process.
Is there documentation that programs are adequately tested for proper functioning when first installed and after any modifications, and that the laboratory director or designee has approved the use of all new programs and modifications?

NOTE: Computer programs must be checked for proper performance when first installed and after any changes or modifications. Any changes or modifications to the system must be documented, and the laboratory director or designee must approve all changes, additions and deletions in programs, the test library, and major computer functions before they are released. Documentation must be retained for at least two years beyond the service life of the system.

COMMENTARY:

N/A

NEW* *03/30/2005*

GEN.43033 Phase II YES , Sada documents any changes that he makes to the FoxPro source code.

Are customized programs appropriately documented?

NOTE: The purpose of the computer program, the way it functions, and its interaction with other programs must be clearly stated. The level of detail should be adequate to support trouble-shooting, system modifications, or additional programming.

COMMENTARY:

N/A

GEN.43044 Phase II YES, Sada is also keeps track of this.
Is there an adequate tracking system to identify all persons who have added or modified software?

COMMENTARY:

N/A

GEN.43055 Phase II This question pertains to the Laboratory N/A YES NO

Is there documentation that all users of the computer system receive adequate training initially, after system modification, and after installation of a new system?

COMMENTARY:

N/A

GEN.43066 Phase II YES, Julie Nassif is on the call list
Is there a responsible person (*e.g.*, Computer System Manager) in the laboratory who is notified of significant computer malfunction?

COMMENTARY:

N/A

*****REVISED**** ***03/30/2005***

GEN.43077 Phase II N/A

Has the laboratory information system been validated for blood banking/transfusion medicine activities?

NOTE: Validation of computers used in blood banking and transfusion medicine is required by the U.S. Food and Drug Administration. The LIS must be validated at initial

installation, and when a change is made to the system. All possible anticipated permutations of processes should be checked (e.g., releasing product to a group-specific patient). Most laboratories utilize a series of screen captures to demonstrate the processes in the LIS. Records of system validation should be retained for at least two years beyond the service life of the system.

COMMENTARY:

N/A

REFERENCES: 1) Department of Health and Human Services, Food and Drug Administration. FDA letter to blood establishments, Mar 21, 1994; 2) Cowan DF, *et al.* Validation of the laboratory information system. *Arch Pathol Lab Med.* 1998;122:239-244.

GEN.43088 Phase II YES, the process is included in the SLI System Policies and Procedures that is being updated.

Is there a documented process to verify the integrity of the system (operating system, applications and database) after restoration of data files?

NOTE: The computer system must be checked after restoration of data files to ensure that no inadvertent alterations have occurred that might affect clinical result reporting. The integrity of the system may be verified, for example, by review of a representative number of computer-generated patient reports, or by generating test ("dummy") patient reports for review. The laboratory director is responsible for determining verification procedure(s) appropriate to the laboratory. Whether or not the data center is located on site, all facilities served by the data center must participate in the verification of the system(s) integrity following a hardware or software failure.

COMMENTARY:

N/A

SYSTEM MAINTENANCE

NEW *03/30/2005*

GEN.43099 Phase II YES, notices are sent to the entire Lab staff by Kristen Pribeck or Jackie Dooley. Downtime is always planned after 4:00 or 5:00 PM.
Is downtime for maintenance scheduled to minimize interruption of service?

COMMENTARY:

N/A

REFERENCE: Valenstein P, *et al.* Laboratory computer availability. A College of American Pathologists Q-Probes study of computer downtime in 422 institutions. *Arch Pathol Lab Med.* 1996;120:626-632.

GEN.43110 Phase II YES, this is also included in the SLI System Policies and Procedures that is being updated
Is there a documented schedule and procedure for regular maintenance of hardware and software either by maintenance contracts or documented in-house procedures?

COMMENTARY:

N/A

***NEW** 03/30/2005*

GEN.43121 Phase II YES, both the servers and network equipment is covered under maintenance agreements. The DPH Network Staff and I have copies of the current maintenance agreements. Sada also keeps track of when the Foxpro system gets re-indexed.

Are service and repair records available for all hardware and software?

COMMENTARY:

N/A

GEN.43132 Phase II YES, the Laboratory is responsible for their printers.
Is there evidence of ongoing evaluation of system maintenance records?

NOTE: Hardware manufacturers have a standard maintenance schedule that must be documented, similar to laboratory instrument maintenance. In addition, regularly scheduled maintenance must be documented for printers (cleaning, other service records).

COMMENTARY:

N/A

SYSTEM SECURITY

The following questions concern unauthorized users. If a system is vulnerable, steps should be taken to prevent unauthorized access.

GEN.43150 Phase II YES, this is also included in the SLI System Policies and Procedures that is being updated. The new electronic access form needs to be included.

Are there explicit documented policies that specify who may use the computer system to enter or access patient data, change results, change billing or alter programs?

NOTE: Policies must define those who may only access patient data and users who are authorized to enter patient results, change results, change billing, or alter computer tables or programs.

COMMENTARY:

N/A

*****REVISED** 03/30/2005***

GEN.43200 Phase I YES, this is also included in the SLI System Policies and Procedures that is being updated. The new electronic access form needs to be included.

Are computer access codes (security codes, user codes) in place to limit individuals' access to those functions they are authorized to use, and is the security of access codes maintained (*e.g.*, inactivated when employees leave, not posted on terminals)?

NOTE: The laboratory should establish security (user) codes to permit only specifically authorized individuals to access patient data or alter programs. A system that allows different levels of user access to the system based on the user's authorization is desirable and usually provides effective security. Examples of best practices include these requirements: periodic alteration of passwords by users; minimum character length for passwords; password complexity requirements (e.g., a combination of alphanumeric characters); recording of failed log-on attempts with user lock-out after a defined number of unsuccessful log-on attempts.

COMMENTARY:

N/A

NEW* *03/30/2005*

GEN.43262 Phase I YES, user workstations are locked to prevented users from downloading unauthorized software, etc… Only the DPH Network and Help Desk Staffs have the ability to load software and change workstation configurations. Are policies and procedures in place to prevent unauthorized installation of software on any computer used by the laboratory?

NOTE: Laboratory computers often serve multiple functions. Many of these computers are connected in a network. The security of the system should be sufficient to prevent the casual user from installing software. Such unauthorized installation may cause instability of the operating system or introduce other unwanted consequences. Many operating systems allow procedures to restrict certain users from installing software.

COMMENTARY:

N/A

GEN.43325 Phase II YES , multiple firewalls separate the Lead Application from the Internet public domain. However, no test results or requests are sent via the Internet.
If the facility uses a public network, such as the Internet as a data exchange medium, are there adequate network security measures in place to ensure confidentiality of patient data?

NOTE: Information sent over a public domain such as the Internet is considered in the public domain. Thus it is potentially accessible to all parties on that network. Systems must be in place to protect network traffic, such as "fire walls" and data encryption schemes. A documented protocol must be in place.

COMMENTARY:

N/A

NEW* *03/30/2005*

GEN.43387 Phase II YES, Lead is a covered entity under HIPAA. Applicable policies and procedures are located on the DPH HealthNet site. Does the laboratory have procedures to ensure compliance with HIPAA?

NOTE: The Health Information Portability and Accountability Act (HIPAA) is a federal law requiring protection of patients' health care information. The law requires maintenance of confidentiality when patient data is transmitted between two organizations. Also, organizations must establish appropriate relationships between sender and receiver of patient data to ensure that the information will be used as intended.

The laboratory must periodically monitor compliance with HIPAA.

COMMENTARY:

N/A

PATIENT DATA

REVISED* *03/30/2005*

GEN.43450 Phase II This question belongs to the Lab N/A YES NO

Is there documentation that all calculations performed on patient data by the computer are reviewed annually, or when a system change is made that may affect the calculations?

NOTE: Errors can be inadvertently introduced into established computer programs. Calculations, algorithms, and/or rules involving reportable patient results must be rechecked and documented to ensure accuracy.

When calculations are performed by an LIS shared by multiple laboratories, this review only needs to be done at one location and each individual laboratory must have a copy of the review documentation. However, any calculations specific to an individual laboratory's methodology must be reviewed by that laboratory and the documentation of that review must be available.

COMMENTARY:

N/A

GEN.43600 Phase I This question belongs to the Lab N/A YES NO

Are system data tables set up to detect absurd values before reporting?

NOTE: Examples of best practices for this step is to check the result against a defined reportable range and critical values for the test, and ensure that the appropriate number of decimal places are present. An audit trail of this process should exist.

COMMENTARY:

N/A

GEN.43750 Phase II This question belongs to the Lab N/A YES NO

Does the system provide for comments on specimen quality that might compromise the accuracy of analytic results (*e.g.*, hemolyzed, lipemic)?

COMMENTARY:

N/A

GEN.43800 Phase II This question belongs to the Lab N/A YES NO

Is there an adequate system to identify all individuals who have entered and/or modified patient data or control files?

NOTE: When individual tests from a single test order (e.g., multiple tests with same accession number) are performed by separate individuals and the test result is entered into the LIS, the system must provide an audit trail to document each person involved. For example, a single accession number having orders for electrolytes and a lipid panel may have testing done by two or more individuals. The laboratory should be able to identify the responsible personnel who performed each test and posted the data. This includes sequential corrections made to a single test result. If autoverification is used, then the audit trail should reflect that the result was verified automatically at a given time.

With point-of-care testing, if the individual performing the test is different than the individual entering test data into the LIS, both should be uniquely identified by the system and retrievable by audit trail.

COMMENTARY:

N/A

REFERENCES: 1) Jones JB. The importance of integrating POCT data into an organized database. *Advance/Laboratory*. 1999;8(9):8-10; 2) Halpern NA, Brentjens T. Point of care testing informatics. The critical care-hospital interface. *Crit Care Med.* 1999;15:577-591.

***NEW** **03/30/2005*

GEN.43812 Phase I N/A
Does the laboratory have a process to ensure appropriate routing of patient test results to physicians?

NOTE: During the course of their medical care in a health care system, the location of a patient may change multiple times; i.e., from various inpatient locations, to outpatient, to physician office patient. The intent of the question is to ensure that patient test results are routed to the responsible physician(s) regardless of patient location. For example, after a patient is discharged from the hospital, test reports should be routed to the physician as well as the hospital medical record.

COMMENTARY:

N/A

GEN.43825 Phase II This question belongs to the Lab N/A YES NO

Are manual and automated result entries verified before final acceptance and reporting by the computer?

NOTE: Data entered into the computer system either manually or by automated methods must be reviewed by an authorized individual who verifies the accuracy of the input data before final acceptance and reporting by the computer. An example of best practices for this step is checking the result against the reportable range and critical values for the test. Depending on the local environment, this may or may not require a second person. Verification procedures must generate an audit trail.

This checklist question does not apply to autoverification procedures (see below).

COMMENTARY:

N/A

GEN.43837 Phase II This question belongs to the Lab N/A YES NO

Are there documented procedures to ensure reporting of patient results in a prompt and useful fashion during partial or complete downtime and recovery of the system?

COMMENTARY:

N/A

REFERENCE: Valenstein P, *et al.* Laboratory computer availability. A College of American Pathologists Q-Probes study of computer downtime in 422 institutions. *Arch Pathol Lab Med.* 1996;120:626-632.

AUTOVERIFICATION

Autoverification is the process by which patient results are generated from interfaced instruments and sent to the LIS, where they are compared against laboratory-defined acceptance parameters. If the results fall within these defined parameters, the results are automatically released to patient reporting formats without any additional laboratory staff intervention. Any data that fall outside the defined parameters is reviewed by laboratory staff prior to reporting.

GEN.43850 Phase II N/A
Is there a policy signed by the laboratory director approving the use of autoverification procedures?

COMMENTARY:

N/A

REFERENCES: 1) Davis GM. Autoverification of the peripheral blood count. *Lab Med.* 1994;25:528-531; 2) Davis GM. Autoverification of macroscopic urinalysis. *Lab Med.* 1999;30:56-60; 3) Nicoli M, *et al.* The use of the Sysmex Co. data processing software program (PC-DPS) for the automatic validation of haematological data. *Clin Chem.* 2000;46:A133; 4) NCCLS. Laboratory automation: communications with automated clinical laboratory systems, instruments, devices, and information systems; proposed standard AUTO3-P. Wayne, PA: NCCLS, 1998; 5) Duco DJ. Autoverification in a laboratory information system. *Lab Med.* 2002;33:21-25.

GEN.43875 Phase II N/A

Is there documentation that the autoverification process was validated initially, and is tested at least annually and whenever there is a change to the system that could affect the autoverification logic?

NOTE: The range of results for which autoverification is acceptable must be defined for all patient tests subject to autoverification.

COMMENTARY:

N/A

***NEW** 10/06/2005*

GEN.43878 Phase II N/A

For all test results subject to autoverification, does the laboratory ensure that applicable quality control samples have been run within an appropriate time period, with acceptable results?

NOTE: This requirement may be met by, 1) the computer system automatically checking quality control status prior to autoverification, or, 2) manually disabling autoverification after any unacceptable QC result, or when QC has not been run within the required time interval.

COMMENTARY:

N/A

***NEW** 10/06/2005*

GEN.43881 Phase II N/A

Are results compared with an appropriate range of acceptable values prior to autoverification?

NOTE: Appropriate comparisons include checking patient results against absurd and critical values requiring manual intervention (repeat testing, dilution, telephone notification of results, etc.)

COMMENTARY:

N/A

NEW* *10/06/2005*

GEN.43884 Phase II N/A

Are results checked for flags or warnings prior to autoverification?

NOTE: The mere presence of a flag may not disqualify a result from autoverification, but any flag that is not specifically recognized by the autoverification program must cause the flagged result to be held for manual review.

COMMENTARY:

N/A

NEW* *10/06/2005*

GEN.43887 Phase II N/A

Does the audit trail in the computer system identify all test results that were autoverified, and the date/time of autoverification?

COMMENTARY:

N/A

NEW* *10/06/2005*

GEN.43890 Phase I N/A

Does the autoverification process include all delta checks that the laboratory performs prior to manual release of test results?

NOTE: This question does not require delta-checking for all autoverified results, but the laboratory's delta-checking procedures should be the same for manually released and autoverified test results.

COMMENTARY:

N/A

NEW *10/06/2005*

GEN.43893 Phase I N/A

Does the laboratory have a procedure for rapid suspension of autoverification?

NOTE: Laboratory personnel should be able to suspend autoverification in the event of a problem with a test method, analytic instrument, or the autoverification program.

COMMENTARY:

N/A

DATA RETRIEVAL AND PRESERVATION

GEN.43900 Phase II YES
Can a complete copy of archived patient test results be reprinted, including original reference ranges and interpretive comments, including any flags or footnotes that were present in the original report, and the date of the original report?

NOTE: Stored patient result data and archival information must be easily and readily retrievable within a time frame consistent with patient care needs.

COMMENTARY:

N/A

GEN.43920 Phase I YES

When multiple identical analyzers are used, are they uniquely identified such that a test result may be appropriately traced back to the instrument performing the test?

COMMENTARY:

N/A

NEW* *03/30/2005*

GEN.43933 Phase I YES, Big Brother system is used. This is also monitored by the DPH Network Staff. Problems documented by the DPH Network Staff.

Does the laboratory have a process to monitor computer system performance, to ensure that the data storage capacity and performance of the system are sufficient to meet the patient needs of the organization?

NOTE: Best practice is to set and monitor thresholds for acceptable storage capacity, average response time and system resource utilization. Laboratory data should be available on-line for a reasonable period of time, which should be determined by the needs of the organization.

COMMENTARY:

N/A

GEN.43946 Phase II YES, this is also included in the SLI System Policies and Procedures that is being updated

Are there documented procedures for the preservation of data and equipment in case of an unexpected destructive event (*e.g.*, fire, flood), software failure and/or hardware failure, and do these procedures allow for the timely restoration of service?

NOTE: These procedures can include (but are not limited to) steps to limit the extent of the destructive event, protocols for periodic backing up and storing of information, procedures for off-site storage of backup data, and protocols/procedures for restoring information from backed up media. The procedures should specifically address the recoverability of patient information. Changes to hardware and software commonly require review and reevaluation of these documented procedures. These procedures must specifically address the physical environment and equipment. This checklist question is often addressed by the organization's disaster plan.

COMMENTARY:

N/A

REFERENCE: Valenstein P, *et al.* Laboratory computer availability. A College of American Pathologists Q-Probes study of computer downtime in 422 institutions. *Arch Pathol Lab Med.* 1996;120:626-632.

GEN.43972 Phase II YES, this is also included in the SLI System Policies and Procedures that is being updated. Included in Network and Server Maintenance Contracts.

Is emergency service for both computer hardware and software available at all necessary times?

COMMENTARY:

N/A

GEN.44000 Phase II YES, this is also included in the SLI System Policies and Procedures that is being updated. UMMS –IT still stores our backup tapes at UMMS in Worcester.

Are storage data media (*e.g.*, tape reels, disk cartridges) properly labeled, stored and protected from damage and unauthorized use?

COMMENTARY:

N/A

GEN.44100 Phase II YES, Big Brother system is used. This is also monitored by the DPH Network Staff. Problems documented by the DPH Network Staff.

Are computer error messages that alert computer users of imminent problems monitored and is the error message response system tested periodically?

NOTE: Computer error messages come in many forms, and usually signify an event that requires immediate attention to rectify a situation. Examples of error messages include system errors, low disk space warnings, database validation errors, exceeding environmental limits, etc. There should be a person responsible for acknowledging the message, a defined system of notification, and response to the situation. The error message response process needs to be periodically tested.

COMMENTARY:

N/A

GEN.44150 Phase II YES, this is also included in the SLI System Policies and Procedures that is being updated

Is there documentation of responses to any error messages during the system backup?

COMMENTARY:

N/A

GEN.44200 Phase II YES, this is also included in the SLI System Policies and Procedures that is being updated

Is there a documented record of unscheduled downtime, system degradation (response time), or other computer problems that includes reasons for failure and corrective actions taken?

COMMENTARY:

N/A

REFERENCE: Valenstein P, *et al*. Laboratory computer availability. A College of American Pathologists Q-Probes study of computer downtime in 422 institutions. *Arch Pathol Lab Med.* 1996;120:626-632.

INTERFACES

GEN.45500 Phase I N/A

If the system uses an interface to populate data into another computer system, is a documented encoding and transmission scheme such as HL-7 utilized?

NOTE: Interface engines allow data from one computerized database to be translated and automatically entered into another divergent system. A documented encoding and transmission scheme should be utilized to accomplish this task. The most common language used at this time is HL-7.

COMMENTARY:

N/A

GEN.46000 Phase I N/A

As applicable, are reference ranges and units of measure for every test transmitted with the patient result across the interface?

NOTE: The reference range, including units of measure, may be specific for a given patient result, and should be attached to that result such that it will be displayed along with the patient result.

COMMENTARY:

N/A

GEN.46500 Phase I N/A

Are acceptable transmission limits established for data throughput by the interface engine, and is this parameter periodically monitored and recorded?

NOTE: One potential bottleneck related to the reporting of results is a backlog of requests to be processed by an interface engine. The laboratory should establish a time tolerance limit for results reporting to the output device. Also, the laboratory should periodically monitor the performance of its reporting systems.

COMMENTARY:

N/A

GEN.47000 Phase II N/A

If data in other computer systems can be accessed through the LIS (*e.g.*, pharmacy or medical records), are there documented policies to prevent unauthorized access to that data through the LIS?

COMMENTARY:

N/A

GEN.48500 Phase II N/A

Is there a documented system in operation to periodically verify that patient results are accurately transmitted from the point of data entry (interfaced instruments and manual input) to all types of patient reports (both paper and video displays)?

NOTE: This includes evaluation of data transmitted from the LIS to other computer systems and their output devices. Reference ranges and comments, as well as actual patient results, must be evaluated. When multiple copies of tables are maintained within more than one computer system, they must be periodically compared to ensure consistency among all copies in use.

This checklist question applies only to interfaces through which laboratory information systems directly send or receive data. For example, if the laboratory information system is interfaced with the hospital information system, the laboratory must verify the accuracy of patient results transmitted across the interface between the two systems. However, the checklist question would not apply to data transmitted from the hospital information system to a physician office information system.

COMMENTARY:

N/A

REFERENCE: Cowan DF, *et al.* Validation of the laboratory information system. *Arch Pathol Lab Med.* 1998;122:239-244.

*****NEW***** ***03/30/2005***

GEN.48750 Phase II N/A

Are there procedures for changes in laboratory functions necessary during partial or complete shutdown and recovery of systems that interface with the laboratory information system?

NOTE: These procedures must ensure integrity of patient test data. Procedures must include verifying recovery of interfaced systems, and replacement or updating of data files, as necessary.

COMMENTARY:

N/A

REFERENCE: Valenstein P, *et al.* Laboratory computer availability. A College of American Pathologists Q-Probes study of computer downtime in 422 institutions. *Arch Pathol Lab Med.* 1996;120:626-632.

NETWORKS

GEN.49000 Phase I YES, Big Brother system is used. This is also monitored by the DPH Network Staff. Problems documented by the DPH Network Staff.

Is there periodic monitoring of network performance and availability to all sites?

NOTE: Networks are the medium of data transport. Periodic review of collision rates, throughput, and downtimes should be conducted to assist in network maintenance and design.

COMMENTARY:

N/A

GEN.49500 Phase I YES

Is the network equipment accessible, well-maintained, and adequately labeled, showing which devices are using a specific port?

NOTE: Cables and ports should be monitored so that a device can be found quickly in case of network failure.